UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,438	07/08/2003	Patricia Ann Jakubik	RSW920030078US1	7454

36736 7590 01/17/2008

DUKE W. YEE
YEE & ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
FRINK, JOHN MOORE	
ART UNIT	**PAPER NUMBER**
2142	

MAIL DATE	DELIVERY MODE
01/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/615,438
Filing Date: July 08, 2003
Appellant(s): JAKUBIK ET AL.

Kevin S. Afghani
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/09/2007 appealing from the Office action mailed 08/12/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0083331	**Krumel**
6,757,255	**Aoki et al.**
6,847,613	**Mimura et al.**
2003/0043740	**March et al.**
7,194,538	**Rabe et al.**

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 – 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krumel (US 2002/0083331 A1) in view of Mimura et al. (US 6,847,613 B2), hereafter Mimura, further in view of Aoki et al. (6,757,255 B1), hereafter Aoki, further in view of March et al. (US 2003/0043740 A1), hereafter March.

3. Regarding claim 1, Krumel shows a method of detecting a denial of service attack at a network server (Fig. 18), including being responsive to the number of packets in a specified interval exceeding a specified minimum [0009-0011, 0071-0073, 0082-0084], and setting a denial of service event marker ([0108-0109]).

Krumel does not show counting the number of inbound packets and a number of discarded packets in a specified interval.

Mimura shows counting the number of inbound packets and a number of discarded packets in a specified interval (col. 7 lines 1 – 16).

It would have been obvious to one of ordinary skill in the art at the time of he invention to modify the disclosure of Krumel with that of Mimura in order to enable collecting and thus displaying more information about current system conditions to users, allowing said users to make more informed decisions.

Krumel in view of Mimura do not show calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, as a response to the number of discarded packets.

Aoki shows calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets (Fig. 10, col. 9 line 12 – col. 10 line 19).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Krumel in view of Mimura with that of Aoki in order to express system information related to packet drops in both rates (as shown by Krumel) and percentages, as the are two inherently related, thus enabling providing information to users in a variety of forms.

Krumel in view of Mimura and Aoki do show being responsive to a number of discarded packets, but they do not show where this response is performing a calculation determining a percentage of discarded packets.

The examiner takes official notice that it was notoriously old and well known in the art at the time of the invention that performing an addition step (inherently involved in the tracking of said number of discarded packets) is simpler logically and computationally than calculating a percentage, which requires more complex multiplication/division.

The claimed 'responsive to a number of packets' inherently involves a simple addition step, as tracking the count of a number of items on a computer inherently utilizes addition. By performing said 'calculating a percentage' responsive to the number of discarded packets, tracked by addition, the simple addition step is performed frequently (each time a packet is discarded) and the complex percentage step is performed rarely (only after a certain number of discards have occurred).

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform said simple arithmetic procedure frequently and said percentage calculating procedure rarely, as that would have the predictable result of lowering processor utilization, thus increasing performance.

It thus would have been obvious to one of ordinary skill in the art at the time of the invention to perform said calculation of a percentage of discarded packets as a response to the number of discarded packets.

Krumel in view of Mimura and Aoki show setting a denial of service marker (Krumel, Fig. 18), and also show monitoring network congestion based on the percentage of discarded packets (Aoki, col. 9 line 63—col. 10 line 15) but do not explicitly show where said denial of service marker is set responsive to the percentage of discarded packets exceeding a specified threshold.

March shows responsive to a percentage of packets exceeding a threshold, a denial of service attack is reported ([97-103]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Krumel in view of Mimura and Aoki with that of March in order to accurately report the occurrence of denial of service attacks.

4. Regarding claim 2, Krumel in view of Mimura, Aoki and March further show collecting inbound packet information to further characterize the denial of service attack (Krumel, [108-109], Aoki, Fig. 10, and, specifically where March shows a 'generate alarm' option that avoids the 'shutdown' option, thus resulting in continuing to gather data (March, Fig. 7, [97-103]).

5. Regarding claim 3, Krumel in view of Mimura, Aoki and March further show initiating a flood monitoring process that is executed at designated intervals to collect the inbound packet information (Mimura, col. 7 lines 1 – 16) while the denial of service attack is in progress (March, [97-103], Krumel, Fig. 18, [108-109]).

6. Claims 4 - 10 rejected under 35 U.S.C. 103(a) as being unpatentable over Krumel in view of Mimura, Aoki and March as applied to claims 1 - 3 above, and further in view of Rabe et al. (US 7,194,538 B1), hereafter Rabe.

7. Regarding claim 4, Krumel in view of Mimura, Aoki and March further show a denial of service marker (Krumel, Fig. 18; Mimura col. 7 lines 1 – 16, Aoki, Fig. 10, col. 9 line 12 – col. 10 line 19) responsive to a number of discarded packets (Krumel [0085,0109], March [0097-0103]).

Krumel in view of Mimura, Aoki and March do not show resetting the denial of service event marker if a number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum.

Rabe shows resetting an alarm after a second specified minimum (in Rabe's case, specified as normal operating conditions) is reached (col. 21 lines 50 – 67).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Krumel in view of Mimura, Aoki and March with that of Rabe to prevent an alarm from sounding incessantly as well as to ensure that said alarm was only active when alarm conditions were present.

Krumel in view of Mimura, Aoki and March and Rabe do not explicitly show where said monitoring is done in the interval before execution of the flood monitoring process. However, Mimura, as described in the response to claim 2, shows monitoring at all intervals (Fig. 7) unless specifically shut down. It thus would have been obvious to monitor for the packet drop rate to return to normal at all times, including before execution of the flood monitoring process.

8. Regarding claim 5, Krumel in view of Mimura, Aoki, March and Rabe further show resetting the denial of service event marker if a rate of discarded packets (Krumel, [0085,0109]) in the specified interval before execution of the flood monitoring process is less than a second specified threshold (Rabe, col. 21 lines 50 – 67, Mimura, Fig. 7, col. 7 lines 1 – 16, Aoki Fig 10).

9. Regarding claims 6 and 10, Krumel in view of Mimura, Aoki, March and Rabe further show collecting the inbound packet information to further characterize the denial of service attack when the denial of service attack is declared over.

Mimura, as described in the response to claim 2 and further in the response to claim 4, shows monitoring at all intervals (Fig. 7) unless specifically shut down. It thus would have been obvious to monitor inbound packet information at all times, including when the denial of service attack is declared over. Furthermore, it is inherent that data collected just before, during, or after a denial of service attack would characterize said attack, as said data would directly reflect on the conditions just before, during and after said attack. Thus continual data collection at all of said intervals would allow additional information regarding said attack to be gathered.

10. Regarding claim 7, Krumel in view of Mimura, Aoki, March and Rabe further show where inbound packet information includes a number of inbound packets in a last interval (Aoki, Fig. 10 and Mimura, col. 7 lines 1 – 16), a number of discarded packets in a last interval (Aoki, Fig. 10) and a packet discard rate (Aoki, Fig. 10).

11. Regarding claim 8, Krumel in view of Mimura, Aoki, March and Rabe further show determining if the denial of service attack is still in progress by comparing the

packets discarded in a last interval with the number of inbound packets (Mimura, col. 6 lines 1 – 16, Krumel [71-73,82-84,108-109]), and maintaining the flood monitoring process if the denial of service attack is still in progress (Rabe, col. 21 lines 50 – 67, specifically showing only turning off the alarm when levels return to normal).

Regarding claim 9, Krumel in view of Mimura, Aoki, March and Rabe further show collecting inbound packet information for the last interval (Rabe, col. 21 lines 50 – 67, Aoki, Fig. 10).

(10) Response to Argument

Regarding claim 1, Applicant argues that the cited prior art, specifically Krumel, Mimura, Aoki and March fail to teach 'responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of serve event marker' and that said cited prior art fails to teach 'responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets.' In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Applicant begins elaborating on the above arguments by asserting that March specifically fails to show 'responsive to the percentage of discarded packets exceeding a specified threshold'. Applicant states that March shows the 'checking the rate of incoming packets against a threshold' but asserts that 'the rate of incoming packets is

not the same as the percentage of discarded packets'. However, despite Applicant's assertion, March is not cited to show 'the percentage of packets' as defined by applicant, but rather March is cited to show responsive to a percentage of packets exceeding a threshold, reporting a denial of service attack. This feature is shown clearly in March in paragraphs 97-103.

March is the last reference cited in relation to claim 1. March alone is not cited to show all the claim language addressed by Applicant in the above argument. Krumel in view of Mimura, Aoki and March are cited to show 'responsive to the percentage of discarded packets exceeding a specified threshold'. Aoki is cited to show 'calculating a percentage of discarded packets' (Fig. 10, col. 9 line 12 – col. 10 line 19). Aoki also uses this percentage of discarded packets as a way to measure network health (specifically network congestion, which a denial of service attack inherently effects (col. 9 lines 5 – col. 10 line 5, specifically col. 9 line 63 - col. 10 line 5). March is then cited to show being responsive to a percentage of packets exceeding a threshold, declaring a denial of service attack. This is clearly shown by March in paragraph 101. It is in view of the other cited art, specifically Aoki, that Applicant's claim language is shown.

Applicant continues arguing the March reference, saying that the rate of incoming packets disclosed by March is different than the percentage disclosed by Applicant, which Applicant states is 'the number of discarded packets divided by the number of inbound packets'. However, March is not cited to show 'the number of discarded packets divided by the number of inbound packets'; Aoki is. Aoki clearly shows this in col. 9 line 63 - col. 10 line 15.

Applicant then argues that Krumel, Mimura and Aoki 'fail to cure the deficiencies of March'. However, the Examiner does not believe there are deficiencies with the March reference, as March teaches what it was cited to teach. Applicant's arguments thus are not persuasive.

Applicant continues, in subheading A.1.ii, to state that 'Krumel, Mimura, Aoki and March fail to teach or suggest the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets'. Applicant continues by stating that a portion of the March reference will be addressed. However, Applicant does not cite passages of March, but instead shows a passage from Aoki. It thus assumed that it was Applicant's intention to refer to the Aoki reference.

Applicant states that Aoki does not teach or suggest the feature of 'responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets'. However, Aoki was not cited to show all of this information. Rather, Aoki was cited to show determining network congestion based on a calculation of the percentage of discarded packets (Aoki, col. 9 line 10 - col. 10 line 10, showing a 'performance index detecting unit' utilizing a percentage of discarded packets). Applicant continues by stating that Aoki fails to show a 'responsive to' relationship regarding the percentage of discarded packets. Again, however, Aoki was not cited to show said 'responsive to' relationship. Thus Applicant's argument is not persuasive.

Applicant continues by arguing Examiner's use of official notice through the use of a small excerpt of Examiner's official notice statement. The Examiner's entire statement and motivation for official notice, which appeared in the previous action, is as follows:

> Krumel in view of Mimura and Aoki do show being responsive to a number of discarded packets, but they do not show where this response is performing a calculation determining a percentage of discarded packets.
>
> The examiner takes official notice that it was notoriously old and well known in the art at the time of the invention that performing an addition step (inherently involved in the tracking of said number of discarded packets) is simpler logically and computationally than calculating a percentage, which requires more complex multiplication/division.
>
> The claimed 'responsive to a number of packets' inherently involves a simple addition step, as tracking the count of a number of items on a computer inherently utilizes addition. By performing said 'calculating a percentage' responsive to the number of discarded packets, tracked by addition, the simple addition step is performed frequently (each time a packet is discarded) and the complex percentage step is performed rarely (only after a certain number of discards have occurred).
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention to perform said simple arithmetic procedure frequently and said percentage calculating procedure rarely, as that would have the predictable result of lowering processor utilization, thus increasing performance.

> It thus would have been obvious to one of ordinary skill in the art at the time of the invention to perform said calculation of a percentage of discarded packets as a response to the number of discarded packets.

To provide a more concise summary, the official notice is essentially stating that it is obvious to avoid frequently performing a complex task (calculating a percentage) by instead performing a simple task (performing addition in order to count packets) and then performing the complex task only as necessary.

Applicant argues that the official notice does not show 'in the specified interval exceeding a specified minimum' aspect of the claim language. However, official notice was not used to show this, rather, Mimura was specifically cited to teach this limitation (col. 7 lines 1-16).

Applicant continues by arguing that 'March fails to cure Krumel, Mimura and Aoki'. However, the Examiner does not believe that Applicant has proven said references are lacking, and thus Applicant's argument is not persuasive.

In subheading A.2, Applicant argues that insufficient reasons to combine the above prior art have been given. Specifically, Applicant repeats the arguments addressed above, without providing any additional reasons that said arguments should be persuasive.

Applicant then states that the reason given for combining Krumel, Mimura, Aoki and March do not support a conclusion of obviousness. To support this argument, Applicant repeats the justification the Examiner gave for modifying the disclosure of Krumel in view of Mimura and Aoki with that of March, which was 'in order to accurately report the occurrence of denial of service attacks', and states that Krumel already

achieves this in paragraphs 116 and 117. However, paragraphs 116 and 117 simply describe an attack alarm; no mention is made regarding denial of service attacks or a denial of service attack alarm. Since Krumel does not in any way address a denial of service alarm or reporting denial of service attacks, Applicant's argument is not persuasive.

In heading B, Applicant begins arguing the reasons for modifying the previously addressed art (Krumel in view of Mimura, Aoki and March) with Rabe. Applicant's specific argument, which begins under heading B.1, repeats the argument from claim 1, stating that claim 4 should be allowable as it depends on claim 1. This is not persuasive for the reasons given above.

Applicant continues by arguing that neither Rabe nor the other cited art teach 'resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum'. More specifically, Applicant acknowledges that Rabe discloses 'resetting an alarm when a value falls below a threshold' but argues that Rabe does not mention a denial of service event marker. However, Rabe was not cited to show a denial of service event marker. Krumel in view of Mimura, Aoki and March were specifically cited in claim 4 to show said denial of service event marker (Krumel showing an alarm in Fig. 18, with Mimura col. 7 lines 1 – 16 and Aoki col. 9 line 12 - col. 10 line 19 and Fig. 10 showing said denial of service event). Since the previously cited art was used to show said denial of service event marker, not the Rabe reference, Applicant's argument is unpersuasive.

Applicant continues by repeating this unpersuasive argument. However, given that Rabe clearly shows resetting an alarm after a specified minimum, which is all Rabe was cited to show (col. 21 lines 50 - 67, where said specified minimum is shown as normal operating conditions) Applicant's argument is again not persuasive.

Applicant then points out that the Examiner noted that the previously cited art does not show all of claim 4. However, this is inherent given that Rabe was cited to make up for any deficiency. Applicant's arguments therefore are not persuasive.

Applicant continues under heading B.2 to state that a proper reason to combine Krumel in view of Mimura, Aoki and March with that of Rabe was not given. First, Applicant argues that Krumel in view of Mimura, Aoki, March and Rabe do not show claim 4, repeating the argument addressed in the preceding paragraphs. This argument is not persuasive for the reasons given above.

Applicant than argues that no sufficient reason for modifying Krumel in view of Mimura, Aoki and March with Rabe was given. The Examiner's reason for combination included 'to prevent an alarm from sounding incessantly as well as to ensure that said alarm was only active when alarm conditions were present.' Applicant then argues that Krumel already provides for this feature. However, Krumel only provides for an alarm that a user may reset by manually pressing an alarm button. This is not the same as Rabe's teaching of resetting an alarm after a specified operating condition has been reached; Rabe teaches an alarm that would be automatically reset after a condition has been met, Krumel teaches simply that an alarm *may* be reset *manually*, and, unlike Rabe, makes no accommodation for stopping said alarm from continuing to sound when

alarm conditions are no longer present. Applicant's argument therefore is not persuasive.

Applicant concludes that the remaining claims should be allowed based on the reasons given for claims 1 and 4. Since the reasons for allowing claims 1 and 4 are not persuasive, this argument is similarly unpersuasive.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

John Frink, 1/07/2008

JMF

Conferees:

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

JASON CARDONE
SUPERVISORY PATENT EXAMINER